WHAT IS YOUR "BIRTHDAY ELLIPTIC CURVE"?

HENG HUAT CHAN, ELISAVET KONSTANTINOU, ARISTIDES KONTOGEORGIS AND CHIK HOW TAN

Dedicated to all those who can have their birthday curves generated without the use of Hilbert class polynomials

Abstract. In this article, Ramanujan-Weber class invariants and its analogue are used to derive *birthday elliptic curves*.

1. Introduction

In 2009 at *Max Planck Institut für Mathematik (Bonn)*, P. Stevenhagen asked the following question :

> "Given any N, can one find a variety and a prime p such that the number of points over the finite field $\mathbf{F}_p$ is N?"

In the case when the variety is of genus 1, we are looking for elliptic curves and a prime number p for which the number of points on the elliptic curves over the finite field $\mathbf{F}_p$ is N. Stevenhagen highlighted a method which allowed him to produce an elliptic curve rapidly if N (more than 60 digits) is given. For more details, see his work with R. Bröker [3].

As an "application" of this work, Stevenhagen mentioned that when N is a birthdate, written as an eight-digit number in the form DDMMYYYY, then one can construct an elliptic curve and a prime p such that the number of points of the curve over $\mathbf{F}_p$ is exactly N. For example, S. Ramanujan's birthdate is 22 December 1887 and the curve

$$y^2 = x^3 + 5887973x + 11302155$$

has exactly 22121887 solutions over $\mathbf{F}_{22130519}$. We shall call an elliptic curve attached to a birthdate a "*birthday elliptic curve*."

Stevenhagen's constructions of such curves require the computations of Hilbert polynomials satisfied by certain special values of the j-invariant. In this article, we illustrate how "birthday elliptic curves" can be constructed with the aid of computer algebra and the Ramanujan-Weber class invariants and their analogues. We **emphasize** here that our method is unlikely to be as powerful as that of Bröker and Stevenhagen. However, the main purpose of this article is to connect Ramanujan's work to the constructions of "birthday elliptic curves" by computing the values of the j-invariant (instead of its minimal polynomials) explicitly using various class invariants.

2. Class invariants

Suppose $n > 4$ is a squarefree integer. Let K_n be the imaginary quadratic field $\mathbf{Q}(\sqrt{-n})$ and C_n be the corresponding ideal class group. It is known, via class field

theory, that there exists a maximal unramified abelian extension of K_n, say H_n, such that the Galois group $\mathrm{Gal}(H_n|K_n)$ is isomorphic to C_n. The field H_n is called the *Hilbert class field* of K_n.

Let

$$j(\tau) = 1728\frac{g_2^3(\tau)}{\Delta(\tau)}, \mathrm{Im}\,\tau > 0,$$

where

$$g_2(\tau) = 1 + 240\sum_{k=1}^{\infty}\frac{k^3 e^{2\pi i\tau k}}{1-e^{2\pi i\tau k}}$$

and

$$\Delta = e^{2\pi i\tau}\prod_{k=1}^{\infty}\left(1-e^{2\pi i\tau k}\right)^{24}.$$

It is known that the Hilbert class field H_n of K_n can be generated by special values of the j-invariant over K_n [7, Theorem 11.1].

The use of special values of the j-invariant to generate H_n is far from satisfactory as their absolute values are often very large. Computing the minimal polynomials satisfied by these values also involved large integers. As such, other class invariants are more desirable. For more details about the disadvantage of using j-invariants, see the paper by Gee and Stevenhagen [8] and the references there.

We collect here a list of class invariants g_n, G_n, t_n and λ_n used to replace j-invariants as functions that generate the Hilbert class fields.

(a) Let $n \equiv 2 \pmod 4$ and

$$g_n = 2^{-1/4}e^{\pi\sqrt{n}/24}\prod_{k=1}^{\infty}(1-e^{-\pi\sqrt{n}(2k-1)}).$$

Then

$$H_n = \begin{cases} K_n\left(g_n^{12}\right) & \text{if } 3|n, \\ K_n\left(g_n^4\right) & \text{if } 3\nmid n. \end{cases}$$

(b) Let $n \equiv 1 \pmod 4$ and

$$G_n = 2^{-1/4}e^{\pi\sqrt{n}/24}\prod_{k=1}^{\infty}(1+e^{-\pi\sqrt{n}(2k-1)}).$$

Then

$$H_n = \begin{cases} K_n\left(G_n^{12}\right) & \text{if } 3|n, \\ K_n\left(G_n^4\right) & \text{if } 3\nmid n. \end{cases}$$

(c) Let $n \equiv 7 \pmod 8$. Then

$$H_n = \begin{cases} K_n\left(2^{-3/4}G_n^3\right) & \text{if } 3|n, \\ K_n\left(2^{-1/4}G_n\right) & \text{if } 3\nmid n. \end{cases}$$

(d) Let $n \equiv 3 \pmod{24}$ and

$$\lambda_n = \frac{e^{\pi\sqrt{n/3}/2}}{3\sqrt{3}}\prod_{k=1}^{\infty}\left(\frac{1-(-1)^k e^{-\pi\sqrt{n/3}k}}{1-(-1)^k e^{-\pi\sqrt{3n}k}}\right)^6.$$

Then

$$H_n = K_n\left(\lambda_{n/3}\right).$$

(e) Let $n \equiv 11 \pmod{24}$ and

$$t_n = \sqrt{3}e^{-\pi\sqrt{n}/18} \prod_{k=1}^{\infty} \frac{\left(1-(-1)^k e^{-\pi\sqrt{n}k/3}\right)\left(1-(-1)^k e^{-3\pi\sqrt{n}k}\right)}{\left(1-(-1)^k e^{-\pi\sqrt{n}k}\right)^2}.$$

Then

$$H_n = K_n\left(t_n\right).$$

(f) Let $n \equiv 19 \pmod{24}$. In this case, we compute $\sqrt{27}/t_n^{12}$ and derive H_n as

$$H_n = K_n\left(t_n^6 - 6 - \frac{27}{t_n^6}\right).$$

Remarks. Some of the above claims with regards to the generators of H_n have not been proved rigorously. For example, the statement $H_n = K_n(2^{-3/4}G_n)$ when $n \equiv 7 \pmod 8$ and $3 \nmid n$ appears to be true but one can probably show that $H_n = K_n(G_n^4)$. Readers might also wonder why we write $H_n = K_n(2^{-3/4}G_n)$ instead of $H_n = K_n(G_n)$ even though both fields are the same. The reason being that $2^{-3/4}G_n$ is a unit when $n \equiv 7 \pmod 8$ while G_n is not. Evaluating units are much easier than evaluating algebraic integers. We use extensively the fact that if $\sigma \in \mathrm{Gal}(H_n|K_n)$ then $\sigma(u)$ is a unit if and only if u is a unit. For more details of such computations, see [4].

The use of units such as $2^{-3/4}G_n$ (when $n \equiv 7 \pmod 8$ and $3 \nmid n$) and t_n (when $n \equiv 11 \pmod{24}$) allow us to compute explicitly the values of these class invariants when C_n is of the form

$$C_n \cong (\mathbf{Z}/2\mathbf{Z})^r \oplus \mathbf{Z}/s\mathbf{Z}, \tag{2.1}$$

where $s = 3, 4, 8$. The restriction on the values of s is due to the fact that we can solve polynomial equation with degree of the polynomial less than 5.

With the explicit values of the various class invariants, we could evaluate special values of j-invariants that generate H_n (see [7, p. 264], [5], [1]). We have

$$\begin{aligned} j\left(\sqrt{-n}\right) &= \left(\frac{2^4}{g_n^{16}} + 2^2 g_n^8\right)^3 \\ j\left(\frac{1+\sqrt{-n}}{2}\right) &= \left(\frac{2^4}{G_n^{16}} - 2^2 G_n^8\right)^3 \\ j\left(\sqrt{-n/3}\right) &= -27\frac{\left(\lambda_{n/3}^2 - 1\right)\left(9\lambda_{n/3}^2 - 1\right)^3}{\lambda_{n/3}^2} \end{aligned}$$

and

$$j\left(\frac{1+\sqrt{-n}}{2}\right) = \left(t_n^6 - 6 - \frac{27}{t_n^6}\right)^3.$$

These relations are derived from the facts that g_n^{12} and G_n^{12} are special values of a modular function of level 2, λ_n^{12} is a special value of a modular function of level 3 and t_n^{12} is a modular function of level 9.

We next show show that the number of integers satisfying (2.1) is finite. We need the following theorem:

Theorem 2.1. *Let $h(d)$ denote the class number of the imaginary quadratic field with discriminant d and let $g(d)$ denote the order of the group of genera. Then*

$$\lim_{d\to-\infty} \frac{g(d)}{h(d)} = 0.$$

For a proof of Theorem 2.1, see [11, p. 394 prop. 8.5].

Corollary 2.2. *The class group cannot be isomorphic to $\mathbf{Z}/2\mathbf{Z}^r \times H$, where H is a fixed finite group, for infinitely many discriminants.*

Proof. Indeed in this case $g(d)/h(d)$ is constant and cannot tend to zero. □

We have done an extensive computer search using magma [12] for discriminants of value $\leq 7 \times 10^5$ and we list them in Tables 1, 2 and 3 for $s = 3, 4$ and 8 respectively.

26	29	38	53	61	87	106	109	110	118	129	157	170
174	182	186	201	202	214	222	231	237	246	247	249	255
262	277	286	298	309	318	339	358	366	370	393	397	411
417	430	451	453	473	493	515	517	533	537	546	565	597
606	610	618	665	669	670	682	685	705	707	714	730	741
753	762	771	813	814	817	826	835	843	861	885	913	930
942	949	966	969	970	973	993	1030	1038	1059	1090	1099	1147
1162	1173	1177	1203	1218	1219	1222	1230	1235	1254	1258	1267	1281
1285	1309	1315	1330	1347	1363	1419	1482	1491	1515	1518	1533	1545
1547	1554	1558	1563	1603	1722	1729	1830	1833	1843	1905	1915	1955
1963	1978	2037	2065	2091	2185	2190	2193	2227	2235	2262	2283	2346
2355	2370	2373	2387	2418	2443	2485	2515	2530	2553	2555	2562	2563
2590	2595	2613	2622	2635	2685	2697	2787	2795	2805	2905	2923	2937
2955	2982	3094	3102	3115	3157	3190	3235	3270	3417	3427	3445	3451
3523	3553	3565	3619	3633	3723	3738	3745	3763	3835	3885	3910	3913
3955	3990	4035	4147	4155	4218	4290	4389	4485	4510	4522	4585	4587
4755	4785	4795	4947	5035	5278	5307	5313	5395	5523	5565	5595	5610
5763	5797	5811	5835	6045	6090	6097	6105	6235	6510	6555	6603	6630
6643	6699	6715	6765	6955	6963	6987	7107	7161	7293	7410	7590	7665
7683	7905	8155	8211	8265	8323	8395	8745	8778	8787	8827	9030	9139
9177	9282	9570	9843	9870	9933	10353	10465	10707	10795	10857	10915	11155
11235	11305	11685	11803	12243	12597	13035	13090	13395	14235	14443	14595	14835
15283	15555	15873	16107	17043	18795	18915	19803	20355	20955	20995	21945	23115
24115	24123	24915	24955	25347	25707	25755	25795	26187	26565	27115	27435	34827
36465	37555	42315	42427	47355	51051	64155	70035	86955	94395			

TABLE 1. Discriminants of the form eq. (2.1) with $s = 3$

14	17	34	39	46	55	65	66	69	73	77	82	97
114	138	141	142	145	154	155	193	203	205	213	217	219
238	258	259	265	282	285	291	301	310	322	323	355	390
418	429	438	442	445	465	498	505	510	553	561	570	598
609	645	651	658	667	690	697	723	742	763	777	793	798
805	858	870	897	910	915	955	957	987	1003	1005	1027	1045
1065	1105	1110	1113	1122	1131	1185	1227	1243	1290	1302	1353	1387
1411	1443	1507	1555	1605	1635	1645	1653	1659	1677	1705	1771	1785
1870	1885	1947	2002	2013	2035	2067	2139	2145	2163	2170	2233	2310
2451	2667	2715	2730	2737	2755	3045	3243	3355	3507	3570	3705	3795
4123	4305	4323	4515	4830	4845	5005	5083	5115	5187	5467	6195	6307
7035	7315	7395	7755	7995	8547	8715	8835	9867	11067	11715	13195	14763
16555	19635	31395	33915	40755								

TABLE 2. Discriminants of the form eq. (2.1) with $s = 4$

41	62	94	95	111	113	137	158	161	178	183
185	221	226	295	299	305	313	337	354	371	377
382	395	399	402	406	410	457	466	469	478	481
501	518	562	573	574	577	579	582	583	589	642
646	663	717	721	745	770	785	786	790	834	862
865	889	903	933	938	939	946	979	994	995	1002
1015	1023	1043	1054	1057	1081	1085	1149	1178	1195	1221
1245	1246	1299	1339	1345	1357	1393	1410	1417	1430	1462
1465	1474	1477	1498	1510	1513	1537	1578	1582	1590	1595
1610	1633	1651	1698	1717	1731	1738	1794	1795	1803	1842
1897	1918	1938	1939	1945	1957	1974	2010	2046	2059	2077
2085	2130	2211	2242	2265	2289	2307	2323	2337	2353	2365
2379	2395	2397	2410	2419	2442	2445	2465	2470	2478	2490
2533	2542	2587	2605	2611	2665	2706	2717	2739	2773	2821
2827	2829	2865	2893	2947	2958	2985	2995	3010	3021	3145
3165	3171	3193	3198	3201	3210	3237	3298	3318	3322	3333
3363	3390	3403	3435	3477	3502	3531	3595	3597	3787	3819
3883	3939	3963	4002	4053	4110	4137	4173	4179	4195	4251
4267	4270	4278	4387	4422	4470	4602	4641	4669	4683	4690
4747	4810	4818	4843	4867	4890	4899	4902	4930	4953	5037
5185	5217	5434	5457	5478	5538	5587	5590	5593	5605	5658
5685	5698	5707	5757	5785	5817	5845	5865	5883	5907	5910
5947	5973	5995	6006	6042	6099	6118	6123	6270	6315	6355
6402	6405	6490	6545	6622	6693	6745	6747	6771	6853	6923
7030	7077	7210	7345	7347	7378	7473	7491	7579	7585	7638
7645	7707	7770	7843	7917	7923	8043	8283	8385	8398	8418
8437	8515	8635	8643	8710	8845	9165	9219	9345	9373	9430
9435	9483	9595	9690	9835	9955	9982	10005	10203	10227	10374
10387	10545	10563	10605	10635	10803	11005	11130	11193	11445	11505
11523	11571	11635	11713	11739	11985	12027	12090	12259	12369	12390
12558	12595	12747	12765	12835	12859	13110	13363	13398	13515	13585
13629	13755	13795	13827	14155	14190	14245	14385	14430	14547	14637
14707	15067	15387	15477	15645	15715	15810	15990	16027	16185	16195
16269	16779	16835	16995	17017	17115	17227	17290	17347	17355	17385
17427	17490	17515	17985	18285	18291	18330	18403	18445	18705	18715
18753	18907	19195	19227	19285	19947	19987	19995	20155	20163	20202
20235	20553	20757	20805	21147	21385	21505	21715	21835	22155	22243
22515	22737	22971	23142	23205	23485	23835	23970	24035	24882	26013
27307	28083	28203	29667	30030	31515	32235	32395	32890	34755	35763
35805	36363	36915	37515	37587	37947	38595	39235	39270	39435	40227
40443	40467	40803	43435	43890	44115	45843	45885	46410	47523	47595
49665	50955	51870	52003	53130	53515	54723	55315	57057	57387	57715
60027	63427	64515	65395	66045	73315	74347	74613	74635	76245	76323
76755	82555	84315	89355	89947	92235	96915	100947	102795	105315	111435
112035	113883	119595	123123	126555	130515	140595	143115	155155	198835	199563
212667	323323	435435								

TABLE 3. Discriminants of the form eq. (2.1) with $s = 8$

3. Finding birthday elliptic curves

It is known that [2, Chapter 8] if

$$4p = x^2 + ny^2,$$

then the number of solutions N_p of $\mathcal{E}_n$ over $\mathbf{F}_p$ is given by

$$p + 1 + \delta$$

where $\delta = \pm x$. In order to construct a birthday curve for a given birthdate b, we set $N_p = b$. Suppose that

$$b = p + 1 - x$$

with $4p = x^2 + ny^2$. Then we must have

$$-ny^2 = (p-1)^2 + b^2 - 2(p+1)b. \tag{3.1}$$

We search for primes $p \in (b + 1 - 2\sqrt{b}, b + 1 + 2\sqrt{b})$ such that the expression

$$(p-1)^2 + b^2 - 2(p+1)b$$

factors into $-ny^2$ with y as large as possible so that we have an integer n such that the class group associated with K_n is as in (2.1). The key point here is that the

suitable values of n are somehow rare but we have many choices of pairs (p, n) that solve (3.1).

We then compute a special value of j-invariant, say j_n,[1] that generates H_n and construct the elliptic curve $\mathcal{E}_n$ be

$$y^2 = x^3 - 3c_n x - 2c_n$$

where

$$c_n = \frac{j_n}{j_n - 1728}.$$

The curve $\mathcal{E}_n$ may or may not have $N_p = b$. When $N_p \neq b$, we search for an ℓ such that

$$\left(\frac{\ell}{p}\right) \neq 1$$

and replace $\mathcal{E}_n$ by the "*twist*" of $\mathcal{E}_n$, say $\mathcal{E}_{\ell,n}$ given by

$$y^2 = x^3 - 3\ell^2 c_n x - 2\ell^3 c_n.$$

4. Examples

We first discuss Ramanujan's birthday curve mentioned in Section 1. In this case, we find that

$$(p-1)^2 + b^2 - 2(p+1)b = -163 \cdot 293^2,$$

where $p = 22130519$ and $b = 22121887$. The corresponding field is K_{163}, which has class number 1. The j_n that we used is then the well-known value

$$j\left(\frac{1+\sqrt{-163}}{2}\right) = -640320^3$$

and this value is all we need to construct Ramanujan's birthday elliptic curve.

We now discuss a more "complicated" birthday curve. We shall use the birthdate of Tom Osler, a mathematician at Rowan University. The birthdate is 26 April 1940. It turns out that with $b = 26041940$ and $p = 26031737$

$$(p-1)^2 + b^2 - 2(p+1)b = -2^6 \cdot 7 \cdot 103.$$

The class number of K_{721} is 16 and

$$C_{721} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}.$$

If we were to use the Hilbert class polynomial, then we would need to construct a polynomial of degree 16. Instead of deriving the Hilbert class polynomial, we compute G_{721} since $721 \equiv 1 \pmod 4$. This is obtained by computing the following identities (see [4] for examples of such computations):

$$\left(\frac{G_{721}}{G_{103/7}}\right)^2 + \left(\frac{G_{103/7}}{G_{721}}\right)^2 = 104 + 39\sqrt{7} + 2\sqrt{5336 + 2018\sqrt{7}} \tag{4.1}$$

and

$$\left(G_{721}G_{103/7}\right)^2 + \left(\frac{1}{G_{103/7}G_{721}}\right)^2 = 384 + 146\sqrt{7} + \sqrt{297731 + 112532\sqrt{7}} \tag{4.2}$$

[1]There are $h(n)$ such values where $h(n) = |C_n|$ but we only need one such value. We obtain this value from Section 2.

We can compute (4.1) and (4.2) because we know that the values on the left hand sides are algebraic integers in a degree 4 extension over $\mathbf{Q}$ (see [4] for more details).

From (4.1) and (4.2), it is clear that we can determine G_{721}^4. We then determine G_{721}^4 modulo p by solving the congruence

$$x^2 \equiv 7 \pmod{p}$$

and using this to derive values of radicals such as $\sqrt{297731 + 112532\sqrt{7}}$ in $\mathbf{F}_p$. This will allow us to determine a value of G_{721}^4 modulo p.

Using the relation between j_{721} and G_{721}, we conclude that over $\mathbf{F}_p$, one of the two curves

$$y^2 = x^3 + 25598199x + 17065466$$

and

$$y^2 = x^3 + 15193287x + 24612553$$

has exactly 26041940 solutions. It turns out that the latter yields the correct number of solutions.

Acknowledgements. The first author is funded by NUS Academic Research Grant R-146-000-103-112. The second and third authors supported by the Project "*Thalis, Algebraic modelling of topological and Computational structures*". "THALIS" is implemented under the Operational Project "Education and Life Long Learning"and is co-funded by the European Union (European Social Fund) and National Resources (ESPA). We also thank Prof. J. Antoniadis for pointing us to Theorem 2.1.

References

[1] B. C. Berndt and H. H. Chan, *Ramanujan and the Modular j–invariant.* Canadian Mathematical Bulletin, **42**, no. 4, (1999), 427-440.

[2] I. F. Blake, G. Seroussi, and N. P. Smart, *Elliptic curves in cryptography*, London Mathematical Society Lecture Note Series, 265. Cambridge University Press, Cambridge, 2000.

[3] R. Bröker and P. Stevenhagen, *Constructing elliptic curves of prime order,* Contemp. Math., **463** (2008), 17–28.

[4] H. H. Chan, *Ramanujan's class invariants and Watson's empirical process.* J. Lond. Math. Soc., series 2, **57**, (1998), 545-561.

[5] H. H. Chan, A. Gee and V. Tan, *Cubic Singular Moduli, Ramanujan's class invariant λ_n and the explicit Shimura Reciprocity Law.* Pacific J. Math., **208** (2003), no. 1, 23-37.

[6] S. Chowla *An extension of Heilbronns class number theorem*, Quart. J. Math. Oxford Ser. **5** (1934) 304307.

[7] D.A. Cox, *Primes of the form $x^2 + ny^2$,* John Wiley & Sons, 1989.

[8] A. Gee and P. Stevenhagen, *Generating class fields using Shimura reciprocity,* Algorithmic number theory (Portland, OR, 1998), 441–453, Lecture Notes in Comput. Sci., 1423, Springer, Berlin, 1998.

[9] H. Hasse, *Zur Geschlechtertheorie in quadratischen Zahlkörpern*, J. of the Math. Soc. Japan **3** No.1 (1951)

[10] E. Konstantinou and Aristides Kontogeorgis, *Computing polynomials of the Ramanujan t_n class invariants*, Canad. Math. Bull. **52** (2009), 583-597.

[11] Narkiewicz, Władysław *Elementary and analytic theory of algebraic numbers.* Third edition. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2004. xii+708 pp. ISBN: 3-540-21902-1

[12] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language,* J. Symbolic Comput., 24 (1997), 235-265.

Department of Mathematics, National University of Singapore, 2 Science Drive 2, Singapore 117543
E-mail address: matchh@nus.edu.sg

Department of Information and Communication Systems Engineering, University of the Aegean, 83200 Karlovassi, Samos, Greece
E-mail address: ekonstantinou@aegean.gr

Department of Mathematics, University of Athens, Panepistimioupolis, Athens 15784, Greece.
E-mail address: kontogar@math.uoa.gr

Temasek Laboratories, National University of Singapore, 5A Engineering Drive 1, Singapore 117411
E-mail address: tsltch@nus.edu.sg